View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by University of Saskatchewan's Research Archive

PRIVACY IN THE AGE OF THE INTERNET

by

Bronwen Elizabeth Russell

THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ARTS

In the
College of Arts and Sciences, Department of Sociology

UNIVERSITY OF SASKATCHEWAN

© Bronwen Elizabeth Russell 2009 All Rights Reserved.

PERMISSION TO USE

In presenting this thesis in partial fulfilment of the requirements for a Master of Arts degree from the University of Saskatchewan, I agree that the Libraries of this University may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by the professor or professors who supervised my thesis work or, in their absence, by the Head of the Department or the Dean of the College in which my thesis work was done. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the University of Saskatchewan in any scholarly use which may be made of any material in my thesis.

Requests for permission to copy or to make other uses of materials in this thesis/dissertation in whole or part should be addressed to:

Head of the Department of Sociology
University of Saskatchewan
Saskatoon, Saskatchewan (S7N 5A5)
Canada

ABSTRACT

This paper addresses the claim that there is “zero privacy” for Canadians on the internet. For the interpersonal computing era 1992 to 2007, the relationship between the three major agents (i.e., individual users, federal government, and business) operating on the internet was examined. Three questions guided the research: how has the popular press educated Canadians about internet privacy? what has been the response of the federal government? how have online companies protected the privacy of Canadians? Content analyses of (a) *Maclean’s* magazine, (b) the Privacy Commissioner's Annual Reports to Parliament, (c) and the privacy policies of the most visited websites were conducted. *Complex Adaptive Systems* theory indicated that privacy is an emergent property arising from the interaction of the agents and that the internet is an environment where the agents' interactions lead to limited privacy.

Dedicated to my family, Dr. Paul J. Russell, Dr. Bonita I. Russell, and Ms. Hilary M. Russell, for supporting my educational journey.

May The Force Be With You

ACKNOWLEDGEMENTS

I would like to acknowledge the following University of Saskatchewan faculty members: Dr. Hongming Cheng, my supervisor, for graciously overseeing this thesis to completion and whose expertise, guidance, and support enriched my work; my M.A. committee members, Dr. Terry Wotherspoon and Dr. Despina Iliopoulou, for their contributions to the theoretical underpinnings of my research; the external reviewer, Dr. Robert Hudson, whose critique of privacy enhanced my understanding of the subtleties of the debate; and finally, Dr. Bernard Schissel, whose initial interest in my topic encouraged me to pursue a study of the internet.

I would also like to acknowledge the support of my family: Dr. Bonita Russell for sharing her experiences with the technology that structured my understanding of the internet and for her financial support; Dr. Paul Russell for helping with my logic; Ms. Hilary Russell for assisting with the data collection and looking after my dog; and Mrs. Elizabeth Chatwin, my grandmother, for following my progress daily.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

1.1 Overview

In 1999, the Chief Executive Officer of Sun Microsystems, an American company specializing in computers, software, and information technology, stated that "[we] have zero privacy anyways" in response to consumer concerns regarding privacy and the internet. His comments highlighted the sophisticated technical systems that existed in the 1990s for monitoring activities on the internet. In the ten years since that statement was made, the level of technical sophistication has only continued to increase. Consider, for example, the *Street View* function of Google Earth – a map generating software program developed by the internet company Google. To create *Street View*, Google cameras scan a street scene to produce an image for the mapping application, and in the process, the cameras inadvertently capture identifying personal information, such as licence plate numbers and recognizable images of individuals on the street (Canadian Broadcasting Corporation, 2007). These maps, with the attached personal information, are then posted to the Google Earth site where a user with a computer and internet connection can view the scenes (Canadian Broadcasting Corporation, 2007).

Despite the seemingly unanticipated impact of software programs like Google Earth on the privacy of citizens, sociologists and other academics with the training and vision necessary to examine privacy and the internet are not contributing sufficiently to this area of research, although according to some sociologists, they should be (DiMaggio, Hargittai, Neuman, & Robinson, 2001:307). For example, the sweeping generalization made by Sun Microsystems' Chief Executive Officer (CEO) that internet users have "zero privacy" needs to be challenged.

The purpose of this thesis was to develop a framework for evaluating this statement; that is, is there (potentially) "zero privacy" on the internet? It is argued that the limits to privacy emerge from the architecture of the internet itself and interactions among the major agents.

1.2 Research Questions

For this thesis, the focus is on changes to personal privacy during the development of the *interpersonal computing era*[1], the period 1992 to 2007, which includes the timeframe covered by the remarks of the CEO of Sun Microsystems. Specifically, the research questions are the following:

(a) How has the popular press educated Canadians about the potential changes in personal privacy associated with the advances in technology?
(b) What has been the political response from the Canadian federal government to the potential changes in personal privacy associated with the advances in technology?
(c) Do the privacy statements on the most popular commercial websites accessed by Canadians protect their personal information?

1.3 Project Overview

A fundamental premise of this paper is that internet privacy is an emergent property of agent interactions in a technical system. The paper proceeds as follows. In Chapter 2, privacy is conceptualized and a working definition is developed. Then, the development of the architecture of the internet is traced in order to understand the relationship between the environment and privacy. In Chapter 3, complex adaptive systems theory is introduced to explain how privacy is conceptualized on the internet. Chapters 4 and 5 describe the methodology and present the results based on content analysis of three data sources. Maclean's and the Privacy Commissioner's Reports provided the data to answer the first two research questions; Alexa media provided the data for the third question.

[1] The interpersonal computing era as defined by Beekman, Quinn & Anderson-Freed (2006) began in the early 1990s and continues through to the present.

CHAPTER 2: BACKGROUND INFORMATION AND LITERATURE REVIEW

The following chapter conceptualizes the research questions in the context of privacy and the internet from several perspectives. The chapter begins with a discussion on privacy which is followed by a discussion on what is meant by internet privacy and how technical developments, including the rise of databases, place limits on privacy. And finally, the existing literature with respect to personal privacy on the internet is reviewed, and the theoretical framework used to guide this research is introduced.

2.1 What is Privacy?

There is no generally accepted definition, or "singular essence", of privacy (Solove, 2008:iv). Westin (2003:431) defines privacy as "the claim of an individual to determine what information about himself or herself should be known to others", whereas Warren and Brandeis (1890:193) define the term as "the right to be [left] alone". The use of the term privacy may also be confused with other related terms such as liberty, autonomy, secrecy, or solitude (Tavani, 2007:3). Robert Post argued that given the number of distinct and competing meanings of *privacy*, using the word at all can be problematic, suggesting that one conceptualization will not suit all circumstances (Solove, 2008:2).

Another concern is which definition will be most influential. The Privacy Commissioner of Canada defines privacy as the protection of collection, use, or disclosure of personal information (Privacy Commissioner, 2008). Further, personal information is defined as "factual or subjective information, recorded or not, about an identifiable individual" (e.g., age, name, income, credit records) but does not include information that can "be found through publicly available information such as the telephone book" (Privacy Commissioner, 2008). Businesses that operate in Canada are required to comply with provincial and federal privacy legislation and the definitions therein. Given this requirement for

compliance, it can be argued that businesses are most likely to define privacy for their business use in keeping with the legislation. However, if a business finds the definition to be overly restrictive it can choose to operate its business in a more favourable legislative environment (e.g., moving internet servers outside of the jurisdiction).

For users, privacy is defined both individually and through interaction with business and government. For example, when users visit social networking websites like Facebook or MySpace, they have a "take-it-or-leave-it" choice regarding their personal information. That is, the user can choose to participate (i.e., provide personal information), or choose not to use the service. Of course, a user may decide to provide incorrect information (e.g., provide an alias) to increase anonymity online. In general, then, structural and organizational forces reduce the ability for individuals to control their personal information (Bennett & French, 2003). That is, when interacting with business and government, users generally have to accept the definition of privacy provided in order to receive the service.

Another approach to understanding privacy, one which tends to mitigate definitional issues, is to address the question posed by Clapham, "what is [privacy] supposed to protect?" which suggests, as other researchers have also noted, that privacy protects different things depending on context (Clapham, 2007:109; Paine, Reip, Stieger, Joinson, & Buchanan, 2007:526; Bannister, 2005:66). For example, when an individual is in a washroom, privacy refers to not being observed by surveillance cameras, and when an individual is in a telephone booth, privacy refers to not being overheard by passersby. Understandably, this contextualization of privacy is temporal. For example, the concept of privacy envisioned by Warren and Brandeis in 1891 was centred on individuals being free from unwanted observation and being able to restrict the circulation of personal information. Over the next 100 years, personal feelings of humiliation and anger have driven the need for privacy rights, resulting in periodic re-examination of what needs to be protected (Clapham, 2007). Today, the right to privacy (a residual right), like all human rights, focuses on maintaining human dignity (Clapham, 2007). And with the advances in communication information technology of the past 25 years, the dimensions of privacy are again being reconsidered. Perhaps the ability to adapt to changing conceptualizations of privacy within society

represents the most powerful aspect of the concept – to remain relevant through adaptation to societal change (Clapham, 2007).

One such adaptation is that required to address the threats to privacy encountered on the internet. In this context, there are four constructs that generally need to be considered. First, privacy in Canada should not be considered as a private/public dichotomy, but rather, as a continuum ranging from clearly private to clearly public. Solove posited that although some personal information is neither intimate nor directly private, that information is not then public (2008:69). In the context of the internet, for example, although a personal email address is not intimate, the address is not automatically considered public. Removing this arbitrary dichotomy between public and privacy may further improve overall societal function, for a continuum of the personal allows for greater freedom to explore social issues (Clapham, 2007).

Second, privacy should be considered not only an individual right, but also a social value because considering it just an individual right "undervalues" the concept within Canadian society (Solove, 2008:79, 89). For when individual privacy "rights" have been violated to protect the greater good, such violations ultimately define the general protection offered to every member of that society (Solove, 2008). For example, the Canadian government is drafting a new wiretap law applicable to the internet (e.g., email). Such legislation, should it pass into law, will fundamentally change how the police monitor Canadians: no longer will the information need to be captured in "real time" (i.e., download a copy from the ISP) and the possibility exists to capture information transmitted in the past (e.g., emails from last month) (CBC, 2009). Privacy allows individuals to develop their beliefs, political opinions, critiques, countercultures, and to experiment outside of the judgement of societal norms (Solove, 2008:80). Accordingly, privacy should be considered in terms of its contribution to society rather than solely as a possession of individuals (Solove 2008:91). In brief, privacy is protected not entirely for the individual's needs, but for the needs of a healthy society and, therefore, should be embedded in social structure (Solove, 2008:92,93).

Third, the question of who controls the personal information collected is an issue evolving from the technical aspects of the internet, an issue germane to the concept of internet privacy (Solove, 2004:167; Solove, 2008:19,24). Often, control is obtained through ownership of the information (i.e., personal information belongs to the identified individual), but in the context of the internet, this definition is not sufficient; rather the question becomes who owns the environmental information (e.g., IP address, CPU size, entry and exit pages, and operating system) collected from users? Solove points out that "individuals are not the lone creators of their web-browsing information, for most of that information is created from the interaction between the user and websites" (2008:27.83).

Fourth, secrecy, or the concealment of information, is related to privacy and of special importance to the internet and internet privacy (Solove, 2008:21). Secrecy highlights the potentially negative aspects of privacy and indicates how privacy can be used to present or preserve an image that may not be consistent with the information available. Within society, the need for privacy must be balanced with the need to prevent harm to society (Solove, 2008:76). However, it is important to recognize that secrecy, as a part of internet privacy, is also relative: secrecy depends on the situation. Internet secrecy can refer to (a) users who use anonymizing software (software that uses a "proxy" public server to mask the user's server) to surf the internet free from adware (software programs that deliver advertisements based on data gathered from cookies on users computers), or (b) to those users who use the same software to post derogatory or inflammatory comments on a webpage message board.

In addition to these four constructs, there are two metaphors to consider -- *Big Brother* and *The Trial*. The dominant metaphor for loss of privacy or the limitations of privacy is *Big Brother* (Solove, 2004:27). *Big Brother*, the totalitarian government portrayed in George Orwell's novel *1984*, is all-knowing and always watchful, a government whose citizens are always under surveillance, or are always under the threat of surveillance (Solove, 2004:7,34). The underlying concept of *Big Brother* is that privacy is invaded by a benevolent power. Sociologist Michel Foucault utilized a *Big Brother* perspective when arguing that "surveillance changes the entire landscape in which people act, leading toward

an internalization of social norms that soon is not even perceived as repressive" (Solove, 2004:35). The metaphor of *Big Brother* has been expanded to include *Little Brother*s, or businesses, referring to the role business plays in monitoring citizens for its own business purposes or for assisting *Big Brother* (Solove, 2004:32). For example, businesses are *Little Brothers* when they turn over their customer data to law enforcement agencies.

There are, however, two limitations to using the Big Brother metaphor to conceptualize privacy on the internet: (a) commercial organizations do not generally collect customer information to aid totalitarianism, and (b) surveillance is accomplished using software programs (dataveillance), meaning there is no direct observation of users by others. Accordingly, Solove argues that with respect to privacy on the internet, *Big Brother* is an incomplete metaphor (2004:27). He suggests a different metaphor, the bureaucracy highlighted in Franz Kafka's *The Trial*. This existentialist novel captures Joseph K's "helplessness, frustration, and vulnerability when a large bureaucratic organization has control over a vast dossier of details about one's life…with little accountability", details that are also "inaccessible" to Joseph K (Solove, 2004:9,36). Instead of conceptualizing privacy as a *Big Brother*-style invasion, the limits of privacy emerge from the architecture of the bureaucracy depicted in *The Trial*. That is, the architecture of the legal system and the relationships between the lawyers, judges, and Joseph K all impact the bureaucracy. Using The Trial metaphor, the limits of privacy are then a result of (a) the architecture of the system itself and (b) the interactions of those involved in the system.

For the present research, the following operational definition of internet privacy, based on the four constructs, *The Trial* metaphor, and modelled on Westin's definition (2003) was used to discuss privacy: internet privacy is *a claim of Canadian society to determine what personal information about its citizens should be known to others*. That is, (a) *a claim of Canadian society* addresses the social values and the structural aspects of privacy; (b) *to determine what personal information about its citizens,* addresses the issue of the dichotomy, suggesting members of a society must decide what personal information is private and to what degree it is private; and, (c) *should be known to others,* addresses disclosure. The term *society* was used in the operational definition instead of a specific

group (e.g., Canadians, Canadian government, or Canadian business) because the relationship between each group on the internet defines the level of privacy (a point made earlier), and this relationship is congruent with a definition of a *society*.

2.2 Review of Technical Developments Related to Internet Privacy

The development of the internet can best be understood in terms of three computing eras: the institutional, the personal, and the interpersonal (Beekman, Quinn & Anderson-Freed, 2006:48). The *institutional* era, beginning in the early 1950s, was characterized by a few large computers operated by computer experts; the *personal* era, beginning in the mid 1970s, by the widespread availability of stand-alone computers for use in schools and offices; and most recently, the *interpersonal* era, beginning in the mid 1990s, by interconnected personal computers (Beekman, Quinn & Anderson-Freed, 2006:48). It should be noted that until the third computing era, most personal computers were not connected to the internet (Beekman, Quinn & Anderson-Freed, 2006:48).

Although the focus of this research is on the interpersonal computing era and the technical (i.e., software and hardware) developments of that period, much of the infrastructure of the internet was in place before 1992. In the institutional era, the first internet system, Advanced Research Projects Agency Network (ARPANET), was created to link defence contractors and military research laboratories across the United States (Schell & Dodge, 2002:25). ARPANET allowed scientists and contractors to advance their respective collaborative work and to experiment with the capabilities of the network itself. By the 1970s, ARPANET was open to non-military organizations, a development which marked the beginning of a publicly available internet, although access was restricted primarily to universities and businesses as personal computers were not yet in widespread use.

The personal computing era began with the introduction of the microprocessor and microchip in the early 1970s, two technical innovations which caused “immediate and radical changes in the appearance, capability, and availability of computers” (Beekman, Quinn & Anderson-Freed, 2006:41). The new computers were smaller, cheaper, and more powerful, allowing them to fit the needs of businesses, educators, and families. The internet

also underwent two noteworthy changes during this era: (a) it became international (i.e., connections established to computers outside the United States), and (b) domain names and email protocols were developed (i.e., two features of the underlying structure of the current internet).

The present interpersonal computing era began with the introduction of software which improved the internet's usability for non-computer experts, rendering the internet accessible to anyone who could "point to buttons on a computer screen" (Beekman, Quinn & Anderson-Freed, 2006:49). This advancement also transformed the internet from a "text-only environment [to] a multimedia landscape" (Beekman, Quinn & Anderson-Freed, 2006:49). Two noteworthy events of this era were (a) the development of URL, HTML, and HTTP[2], the backbone technologies of the World Wide Web, and (b) the appearance of commercial providers selling individual access to the internet (Beekman, Quinn & Anderson-Freed, 2006).

It was during the interpersonal era that personal privacy became an issue for four main reasons. First, the number of internet users grew faster than the control systems being put in place to protect users. Second, computer processing and storage space increased substantially, leading to the development of large, integrated databases of personal information that could be easily collected, stored, and searched. Third, and related to the previous issue, personal data was commodified. Finally, advanced end user computing tools became widely available, leading to the rise of viruses and other sophisticated malicious software (Beekman, Quinn & Anderson-Freed, 2006:49).

Considering the four reasons in turn, first, the number of internet users grew exponentially during the interpersonal area: in 1994 the internet had 3 million users worldwide; by 2003, there were 580 million users; and by 2008, 1.4 billion users (Beekman, Quinn & Anderson-Freed, 2006:49; Internet World Stats, 2008). With the increasing number of non-computer experts using the system, new users were unaware of the risks of the inherently insecure

[2] URL (universal resource locator) is the unique address of each internet document; HTML (hypertext mark-up language) is the computer language used for coding and displaying hypertext documents; HTTP (hypertext transfer protocol) presents the rules for linking hypertext documents.

system. Further, with more users, malicious software attacks damaged more computers, and obtaining information from the internet (e.g., personal information or business information) became more economically viable.

Second, *databases* are composed of tables of related information and can be as straightforward as an Excel spreadsheet of bake-sale volunteer names and addresses (i.e., an application requiring one table) or as complex as an airline reservation system containing many interrelated tables (Beekman, Quinn & Anderson-Freed, 2006:267,268,279). Computerized databases are used for (a) storing large quantities of information, (b) organizing and reorganizing information, (c) distributing print or email information, and (d) retrieving information quickly (Beekman, Quinn & Anderson-Freed, 2006:267,268).

Databases were first developed by governments to collect and store information concerning their citizens, but it was business that later drove their use (Solove, 2004:16). Business owners in their early attempts to understand their customer needs, used techniques such as mass marketing, but these techniques were expensive and reached more than the target group. To increase efficiency, marketers in the 1970s started using demographic data to refine direct marketing techniques, a change made possible because computer databases made collecting and using demographic data easier. Since the 1970s, these databases have grown to contain a sizeable collection of customer profiles, a collection that can often represent the most valuable property a company owns (Solove, 2004:19).

Data-mining in a database, or the "discovery and extraction of hidden predictive information" using statistical procedures and artificial intelligence technology, is an additional privacy concern (Beekman, Quinn & Anderson-Freed, 2006:282). An organization using data-mining techniques can expose previously unknown relationships among data. For example, a grocery store chain using data-mining found that the men who bought diapers on Friday nights at their stores also purchased alcoholic beverages (Larose, 2005). Another technique applied to databases is referred to as *aggregation* or the "combined bits and pieces of data…to form a portrait of a person" (Solove, 2008:118). The portrait is obtained by combining individual pieces of information gathered at different

times or places into one aggregate report. For example, combining demographic data with credit rating information and purchase history provides a better picture of an individual's financial status. Data aggregation, like that pointed out in the above example, occurs because many internet websites subscribe to "DoubleClick", a type of information collection software program that consolidates all the different cookies (parcels of text that uniquely identify users) from various websites to create a more complete profile of an individual (Solove, 2004:24). Data-mining and aggregation techniques are a privacy concern because the individuals profiled do not realize or are not informed that various data banks may be accessed to profile them.

Because the internet supports collection technologies like those described above, it has enabled "unprecedented" amounts of information about users to be gathered, combined, analyzed, and stored by third parties, an activity which leads to a reduction in the ability for users to control their personal information (Bannister, 2005; Hinduja, 2004; Solove, 2004:167,216). Any one piece of personal information stored in the database does not necessarily reflect a privacy problem; rather, it is all the pieces that combine to form an aggregate profile of the individual, with the result that "the whole is greater than the sum of its parts" (Solove, 2008:117). For example, as suggested earlier, several databases provide a more accurate profile of an individual than any of the databases separately. However, it was only with the increasing processing capacities of computers and the increasing amount of data transferred to them that techniques like data-mining became viable.

Third, data, specifically consumer data, have become one of the new currencies of modern western society (Beekman, Quinn & Anderson-Freed, 2006:286). For example, one analysis of 15,000 marketing databases found that the databases contained personal information on about 2 billion individuals, including details such as age, income, and political affiliation (Beekman, Quinn & Anderson-Freed, 2006:286). This information can be obtained as the result of an exchange between a customer and a merchant. For instance, a customer obtains a discount at a grocery store in exchange for using the store's computerized customer card, a transaction which the merchant can then use to track the customer's purchases in a marketing database. This example illustrates that as personal

information becomes useful for a business (e.g., for improving business service or targeting advertising), it is commodified, and its value is no longer social or personal; rather, it becomes a commercial asset. This commodification raises three concerns: (a) who, the individual or the company, controls the information? (i.e., ownership), (b) what laws, national or international, protect the personal information?, and (c) what kinds of information may be collected? Further, when data are commodified, they need to be stored where the information is easily accessible, for example, in a database.

Finally, the introduction of end-user software (e.g., JAVA) gave general users uncontrolled access to powerful programming tools, tools that in the past would have required a computer programmer's level of knowledge to execute. It is this software which can be used to create damaging malicious software.

2.3 Literature Review

Much of the research that has been conducted on internet privacy has been the work of academics in disciplines other than sociology (especially business, law, and computer science) and has focused on (a) the relationship between specific attributes and/or behaviours and privacy concerns and (b) the privacy policies of internet businesses (DiMaggio et al., 2001).

An example of the first type is the work of Miyazaki and Fernandez, (2001) who surveyed 162 adults' risk perception and internet experience related to online shopping activity. Internet experience, in this research, was measured using two indicators: duration (number of years/months of regular internet access) and frequency (number of times per month the world wide web was accessed). The authors found an inverse relationship between internet experience and perceived risk regarding online shopping transactions (i.e., increased levels of internet experience led to lower perceived risk) but a positive relationship between internet experience and general privacy concerns (i.e., greater internet experience leads to higher levels of concern). Further, Paine, Reip, Stieger, Joinson, and Buchanan (2007) found that *gender* was not statistically significant in explaining *privacy concerns*; however, another variable, *age*, was positively correlated with *privacy concerns*. Interestingly, and

unlike Miyazaki and Fernandez research, there was no significant relationship between *years of experience*, *hours spent online*, and *privacy concerns*. Paine et al. (2007) also found that participants were concerned about privacy online but were unable to take precautions because they were unsure of how to increase online privacy.

With respect to the second area of research, privacy policies, the focus has been on the content of privacy policies posted on internet websites. In a four year longitudinal study, Milne and Culnan (2002) evaluated the privacy policies of 30 high-traffic American websites (e.g., FedEx and Citibank websites). They concluded that although there was an increase in the number of privacy polices and disclaimers posted over the period of the study, there was no way to determine if the companies involved were actually complying with the posted statements (Milne & Culnan, 2002). A second study by Graber, D'Alessandro, and Johnson-West (2002) analyzed the reading ease of privacy policies posted on American health related websites. The authors concluded that on average two years of college education were needed to understand the policies. A telephone survey of 1,000 American adults by Culnan and Armstrong (1999) investigated whether a privacy statement posted by a web-based company would convince people to share personal information. The authors found that when individuals are informed about how their information is to be used, privacy concerns are alleviated. Additionally, a study by Hui, Teo, and Lee (2007) assessed how consumers respond to privacy statements posted on websites collecting personal information. A field experiment was conducted in which participants answered an online survey; some respondents received a survey with privacy assurances and some received a survey without privacy assurances. The authors analyzed the amount of personal information reported by respondents under each of the conditions and concluded that individuals provide more personal information when presented with privacy assurances (Hui, Teo, & Lee, 2007). And finally, a study by Lauer and Deng (2007) of 269 American undergraduates found that trust in an online company was dependant upon the perceived respect for consumer/user privacy expressed in the company's privacy policy. Trust, according to the authors, is important for successful online business transactions (Lauer & Deng, 2007).

In summary, internet privacy is an emerging area of inquiry that to-date has focused on how users interact with the system for primarily commercial purposes. The challenge for researchers concerned with understanding more complex interactions is explaining the dynamic properties of such interactions, a task for which Stacey (2007) and his Complex Adaptive Systems theory offers some analytic tools. Part of the challenge of understanding internet privacy is to determine how the internet interacts with those who use it (e.g., business, government, or users) and how it changes during these interactions.

2.4 A Complex Adaptive Systems Theory and the Internet

The Information Age (late 20th century) refers to a type of networked society of which the internet is a part (Castells, 2000:695; Beekman, Quinn, & Anderson-Freed, 2005:51). Networks are not a new form of social organization, but older networks could not "manage complexity beyond a critical size" in the way new systems can (Castells, 2000:695). Although network analysis has been the most common approach to understanding social structures, traditional network analysis misses the relational meanings within a network (Emirbayer, 1997:300). That is, additional meanings concerning networks arise from a concept's "place" in the system (Emirbayer, 1997:300).

To interpret the network society, Castells suggests that sociologists (a) re-conceptualize how they understand networks, appreciating that networks can exist without centralized power or hierarchies, and (b) use the new analytical tools (e.g., "computer-based system analysis of dynamic networks") to describe the nonlinear dynamics observed in such networks (Castells, 2000:696,698). He posits that sociologists will have to develop "through synergy among relevant theorizing, computational literacy, and sociological imagination" a new way of understanding these networks (Castells, 2000:698).

One theoretical model that incorporates the relational approach suggested by Emirbayer and the dynamics suggested by Castells is complexity theory. The theory offers new conceptual tools to understand the "diversity of modernity" and an alternative way to conceptualize connections within systems (Walby, 2003:11,13). This inter-disciplinary theory (forms of complexity theory are used in business, economics, mathematics, and biology) provides the

"concepts, methods and epistemology" needed to understand the society emerging from the Information Age (Walby, 2003:11). Further, complexity allows for the study of the system with an "anti-reductionist analytic strategy", meaning the theory works at the macro level without denying individual agency (Walby, 2003:11). In addition, complexity theory does not assume hierarchical forms within interconnections, an assumption allowing for a more flexible approach than traditional network theories utilized by Parsons or Marx (Walby, 2003:14). A hierarchical system is one in which those with power or higher positions (e.g., bosses) control the changes to the system. However, Stacey (2007:111) argues that hierarchical change of any entire system is not possible; instead, change occurs through the local-level interactions. By expanding analysis from a hierarchical approach, researchers can understand how other types of interactions lead to system change.

In order to apply this theory to the internet, it must first be determined if the internet displays the features of a *complex system*. A complex system refers to a system that is comprised of a number of interconnected elements which change over time (Stacey, 2007). Weather prediction is an example of such a system where many interconnected elements (e.g., temperature, air pressure, wind speed, wind direction, and humidity) create a dynamic system, one where specific outcomes are not easily predictable in the long term. Like the weather system, the internet is constructed from many interconnected parts: the physical network of fibre, routers, and servers connecting computers around the world, billions of interconnected web pages, and a billion users.

There are two general criteria for a complex system to qualify as a CAS: first, the system must be constructed from a large number of agents acting in accordance to a set of rules, and second, the interactions between agents must produce orderly patterns (Stacey, 2007). The internet displays these two criteria because, (a) there are a large number of agents and their use is constrained by a set of rules, and (b) the interactions between the agents produce recognizable patterns. The observation that there are 1.4 billion users of the internet and every webpage they visit has a URL (universal resource locator), which gives the location of the specific page, supports criterion one, and the *Power Law of Distribution*, which can

predict the growth rate of a website using current size, growth, and number of links, supports criterion two (Howe, 2002).

There are four additional characteristics used to identify complex systems: self-organization, non-linearity, chaos, and emergent properties (Stacey, 2007). Self-organization is defined as a system where "the whole is required before the parts can have any function, and the parts must be designed" before the system can function (Stacey, 2007:31). That is, the system develops, or organizes, as a whole, gaining complexity during this organization. Self-organization may be traced to the work of Immanuel Kant who questioned how a complex system could develop if the parts must have been pre-designed, thereby implying that the "notion" of the final (or current) system has already been formulated (Stacey, 2007:31). Kant postulated that a complex system would need to start as a simpler system, and the causal development would be formative (rather than transformative) towards the current complexity (Stacey, 2007:31,32). Web pages that are linked to one another are an example of a self-organizing network. Characteristically, complex systems cannot be reduced to their independent elements without destroying the integrity of the system; that is, the elements themselves are too highly integrated to be separated into discrete parts (Stacey, 2007).

Non-linearity refers to the elements or events that are not necessarily connected by time or space but lead to new or changed elements within a system, which in turn, affect the original elements (Stacey, 2007). Further, "one variable can have more than proportional effect upon another" within a non-linear system (Stacey, 2007:13). For example, Wikipedia, the online encyclopaedia, has developed non-linearly. The hosting of Wikipedia, a public web page, led to a complex system of 10 million articles written by volunteers, which are open to revision by anyone with access to the site.

In an ordered or linear system, the next developmental step is reliably predictable based on knowing the history of the system. However, in a non-linear system, the further the predictions are projected onto future steps, the greater the likelihood the prediction fails, even with extensive historical knowledge (Stacey, 2007). For example, on the internet, the

progression from telephone internet connections to wireless internet connections was a non-linear technical development because the technology supporting telephone/cable connections was not a precursor to wireless technologies.

Small events or historical events can have a significant impact on the development of, or changes to, a complex system. For example, the design of the world wide web, which was originally rejected by the computer science establishment as "too simple, was the work of one computer programmer" (Beekman, Quinn & Anderson-Freed, 2006:222). The uncertainty in prediction resulting from the multitude of interconnections is known as chaos. Chaos is useful for understanding the complex behaviours of systems which appear random but are actually governed by the deterministic properties of the system (Pekka, 1999). Further, the actual outcomes of chaotic systems are referred to as emergent properties or patterns, that is, the unpredictable, yet logical, outcome of changes to complex systems. In a chaotic system there are two underlying assumptions: (a) an underlying order exists, and (b) small events or perturbations can cause complex changes or events.

A classic example of a chaotic system is the *butterfly effect*. In this case, the suggestion is made that because a chaotic system is sensitive to initial conditions, when a butterfly flaps its wings in Brazil, it causes a small perturbation in the atmosphere that results in a tornado (the emergent property) in Texas (Pekka, 1999). On the internet, the "butterfly effect" can be seen with the introduction of the world wide web. That is, a file sharing system originally reserved for experts has evolved into a global, multi-media system accessed by millions of people every day.

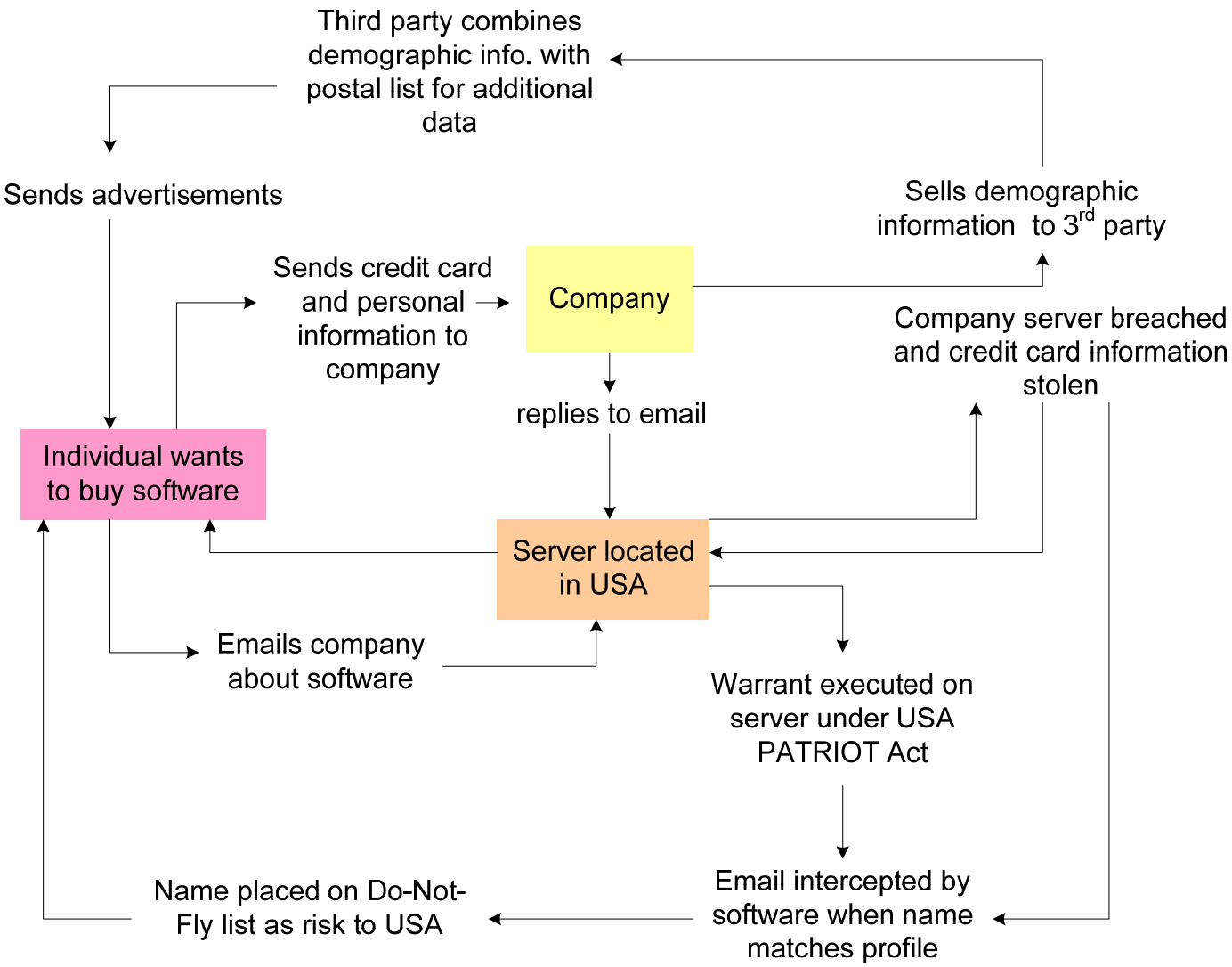
The underlying order of a complex system refers to the spatial patterns (or fractals) that emerge from such systems (Stacey, 2007:183). According to Stacey (2007:183), recognizable patterns can emerge from a complex system, but these patterns are "chaotic" in nature as they can be either stable and regular, or unstable and irregular at any given point in time (Stacey, 2007:183). Such emergent patterns are an indication of an underlying, or deep, dynamic structure. For example, a sand dune is relatively stable most of the time, but when the wind comes up, the sand dune becomes unstable. When the wind subsides, the

sand dune will re-stabilize in a new pattern that could not have been predicted from its original form. In a system not in equilibrium (or in balance), small changes escalate within the system causing enough instability to radically change the system (Stacey, 2007:192). This type of system is difficult to understand using traditional structural theorizing, such as that of Talcott Parsons, whose theorizing is based on systems maintaining equilibrium with their environments (Holton,2006:155). Accordingly, it becomes difficult to use classical structualist theory to understand dynamic systems as predictions cannot be made based on knowledge of the agents involved or their structure within the present systems -- there is no system "blueprint" (Stacy, 2007:193,196).

Viewing the internet as CAS allows the principles of this theory to guide privacy conceptualization in the internet environment. In this environment, the different agents (i.e., government, business, and users) are acting in parallel, constantly acting and reacting to what the other agents are doing, an indication that the world wide web can be seen as a "giant, loosely woven, constantly changing document created by thousands of unrelated authors and scattered about in computers all over the world" (Beekman, Quinn & Anderson-Freed, 2006:21). The controls for this system tend to be highly dispersed and decentralized (i.e., there is no central authority controlling the internet's development), and the overall behavior of the system is the result of every decision made every moment by many different agents (Stacey, 2007).

This decentralization of control, along with the influence of different agents, affects internet privacy. Figure 2.1 presents a simplified example of how privacy is affected by the interactions between agents operating on the internet. Specifically, the figure shows the ways personal information is obtained and used through interaction with other agents.

Figure 2.1: Example of Privacy Issues that May Arise Through Agent Interactions



In summary, privacy, including internet privacy, is a term that eludes a definitive definition. That is, since a "complete" definition of privacy cannot be constructed, an operational definition, developed earlier, serves to guide the interpretation of the research data. For this research, internet privacy is considered a social value not an individual right, and it exists on a continuum depending on context. The technical developments of the internet beginning in the 1970s have shaped the way privacy has been constructed. The existing literature on the internet has focused on a limited number of user interactions for commercial purposes. Complex adaptive systems theory was offered as an explanation for how privacy has been

constructed on the internet. This theory accommodates the technical developments and allows for a structural analysis of the interactions among agents and will be used to interpret the results of the data analysis. It is important to note that without this theoretical construct, issues of privacy cannot be fully understood, for it is the architecture of the internet and the mechanisms by which it is has evolved over time that influence privacy. Chapter 3 explores the nature of the technical environment.

CHAPTER 3: TECHNOLOGY, PRIVACY AND THE INTERPERSONAL COMPUTING ERA

To understand privacy in the interpersonal computing era requires an appreciation of the technical environment, and how the environment has changed over the period between 1989 and 2007. Figure 3.1 presents a timeline of the major developments. Although this research focused on the interpersonal computing era for the years 1992 to 2007, several key technical developments important to internet privacy occurred just prior to 1992. The timeline was extended back to 1989 to include these developments.

An assortment of print and electronic sources was used to construct the timeline. A technological advance was included if it (a) impacted the structure of the internet or computer systems, and (b) related to privacy. Supplemental academic sources on privacy in the modern technical society were examined for major technical advances in the internet for the period 1989 to 2007 (Beekman, Quinn & Anderson-Freed, 2006; Solove, 2004; Solove, 2008; Schell & Dodge, 2002). When an issue was technically complex or was a specialized problem, it was further examined using internet sources. For example, processor speed specifications for Intel processors were obtained from the company's website.

Seven general categories of technical development are shown: search engines, operating systems, storage, web browsers, CPU, laptops, end user software and connectivity. The timeline was used to identify four specific types of advancements that are pertinent to this research: (a) processors, processing speed, and miniaturization, (b) operating systems, (c) advanced end user software, and (d) connectivity.

The processor, or CPU, is the component in a computer that executes programs. The faster the CPU, the more complex the programs the computer can execute. The timeline indicates

that speed increases from Pentium I (300 MHz), through Pentiums, II (450 MHz), III (1.4 GHz), and 4 (3.8 GHz). As well, portable storage size increased as the size of programs (resulting from increased complexity) increased. Prior to 1990, portable storage devices took the form of diskettes, or "floppies" and held only a few megabytes[3] (MB) of data. Later storage devices, such as the zip drive (1994), held 100 MB, increasing to 250MB and 750MB; CD-RW (Compact Disc Read/Write), introduced in 1997, held 650 to 700MB; DVD-RW (Digital Video Disc Read/Write), introduced in 2002, held 4 to 8GB; and USB (Universal Serial Bus) flash drives, first introduced in 2000, hold up to 64GB. As storage size increased, the physical size of computers and storage devices decreased; for example, the Apple iBook (2003) weighed 2.2kg, whereas the Macintosh Portable (1989) weighted 7.3kg. With the decrease in physical size, the ability to keep computers, their storage devices, and the data stored on these devices secure also decreased. Because storage devices are physically small (e.g., can fit on a key fob) but can hold large amounts of information, the risk to privacy associated with the loss of such devices increases. And there is anecdotal evidence for this decrease in security. For example, on PAWS, a University of Saskatchewan web portal enabling students to access university services, there are often postings from students who have lost (or found) USB storage devices on the University campus.

Operating systems (Blue text on Timeline, Figure 3.1) manage the interface between the user, the application or program, and the hardware of the computer. The advantage of the single operating systems of the 1990s was that they could be installed on a variety of different computers, allowing software to be easily shared between users. Concomitant with these operating system and software developments came changes in the threats to privacy. As software developers rapidly produced new operating systems for market (i.e., Microsoft released a new version of its Windows operating system every few years), the systems were not fully tested and *holes*, or errors, in the programming could be exploited, thereby putting personal privacy at risk. For example, Windows 95 was released in 1995;

[3] A byte is 8 bits (or 8 binary units of the smallest unit of information a computer processes). Bytes are further classified as kilobyte (KB or 1000bytes), Megabyte (MB or 10^6bytes), Gigabyte (GB or 10^9bytes) and Terabyte (TB or 10^{12}bytes)

the first virus (a malicious program that damages computers) that exploited weaknesses in Windows 95 appeared a year later (See Timeline, Figure 3.1).

The term *end user software* refers to complete software packages released to internet users (Pink text on Timeline, Figure 3.1). Java (1995) is a programming language for software development that is straightforward and easily transferrable to different platforms. Early viruses designed using such end-user software were developed with the purpose of damaging the computer hard-drive; later viruses were designed to covertly copy and transmit computer records. As mentioned earlier, the introduction of end-user software gave general users uncontrolled access to tools which once would have required a computer programmer's level of knowledge to execute.

Changes in connectivity and access points to the internet also affect privacy (Diffie & Landau, 2008). The early internet system had few agents and few access points, two features which offered structural protection to the data since access was limited. However, as the number and types of connections grew (e.g., dial-up, DSL digital subscriber line, or wireless) so did the opportunity for privacy violations. For example, early wireless signals were analogue and were easily captured using basic radio techniques; further, the method of capturing the signals was not covered by existing wiretap laws (Diffie & Landau, 2008). In addition, the data transfer speed for different types of connectivity varied (dial-up generally transfers data in KB/s while DSL transfers in MB/s), indirectly affecting internet privacy. For example, a dial-up connection that cannot easily transfer large files because of the limits of the line speed does not present the same privacy risk as a DSL connection where large files can be transferred much more quickly.

Figure 3.1: Timeline

The discussion to this point has traced the technical developments of the interpersonal computing era and the impact of each of these developments on privacy. It is clear that privacy on the internet is both technical and interactive. The technical environment shapes the structure in which the agents interact, and the interactions of the agent shape the technical environment. It is not possible to consider privacy on the internet independent of the technical architecture.

CHAPTER 4: METHODOLOGY

4.1 Overview

Based on the argument that a) complex adaptive systems theory can guide privacy conceptualization in the internet environment, b) interactions between agents on the internet influence personal privacy, and c) these interactions are computer-mediated text-based interactions, content analysis was determined to be the most efficacious approach for examining internet privacy. Such an analysis "emphasizes the way versions of the world, society, [and] events…are produced" (Bryman and Teevan, 2005:344).

For the first research question, *How has the popular press educated Canadians about the potential changes in personal privacy associated with the advances in technology?*, Maclean's magazine was the information source. Mass media, such as Maclean's, are acceptable sources of data for social analysis (Bryman and Teevan, 2005:128). Maclean's was chosen because it is (a) a general audience publication, and (b) it represents itself as "Canada's only national weekly current affairs magazine" (www.macleans.ca). It is important, however, to acknowledge that the authors and/or publishers of this magazine may have presented Canadians with a particular view (i.e., bias) with respect to what constitutes newsworthy internet privacy issues. To identify a possible Maclean's reporting bias, the results of the magazine analysis were compared to the timeline entries, a comparison that identified whether the Maclean's articles reflected actual changes in internet privacy concerns or only the *newsworthy* changes.

For the second research question, *What has been the political response from the Canadian federal government to the potential changes in personal privacy associated with the advances in technology?*, the Privacy Commissioner's Annual Report to Parliament for the years 1992 to 2007 served as the data source. The mandate of the Privacy Commissioner is to oversee compliance with the Privacy Act (1983) and Personal Information Protection and

Electronic Documents Act or PIPEDA (2001) and to protect the privacy rights of Canadians granted by these laws (Office of the Privacy Commissioner of Canada, 2007). The reports were chosen to examine the relationship between the concerns of Canadians and the response of the federal government. Other researchers (e.g., Foley, 2007) have used official sources such as government documents when investigating internet privacy issues.

For the third research question, *Do the privacy statements on the most popular commercial websites accessed by Canadians protect their personal information?*, the privacy policies posted by business organizations on high traffic websites were the data source. Privacy policies have been used as a data source by other researchers (e.g., Graber et al, 2002). The high traffic sites were identified using Alexa media, which creates a list by counting the number of Canadian users on its network who visit a particular site. However, the internet activities of all Canadian internet users are not captured by Alexa. To compensate for this limitation, a large sample size (N=100) was used to obtain a representative cross section of privacy policies from a range of websites. The sample was restricted to English language, non-pornographic websites, a requirement which reduced the sample size to 77. Regarding the first restriction, because the researcher is unilingual, only websites with privacy policies written in English were analyzed. Future research could consider websites with policies written in other languages. Pornographic websites were not included because they presented unique privacy issues (e.g., with respect to content or age restrictions), which were not part of this research.

In order to evaluate the differing privacy statements, a standard was required. The Personal Information Protection and Electronic Documents Act (PIPEDA) was chosen because all business operating in Canada are required to comply with the provisions of the legislation. Schedule 1 of the Act -- Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information -- outlines what the obligations of an organization are regarding the personal information of Canadians (Knight, Chilcott & McNaught, 2006). Schedule 1 presents the ten essential action elements, the specific measures of personal information protection, that must be afforded to Canadians by

commercial organizations. These ten elements are the following: accountability; indentifying purposes; consent; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access; and challenging compliance (See Table 4.1 for the definitions of the ten elements). To assess the privacy protection of Schedule 1, each of the clauses within each of the action elements of the schedule was converted into measurable concepts, based on the definition of privacy presented earlier. Appendix 1 lists the Schedule 1 clauses and the associated measurement criteria (See Appendix 1).

Table 4.1: Elements of Schedule 1 and their Definitions (PIPEDA, 2001)

Element	Definition
Accountability	An organization is responsible for personal information under its control and shall designate and individual or individuals who are accountable for the organization's compliance.
Identifying Purposes	The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
Consent	The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
Limiting Collection	The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
Limiting Use, Disclosure, and Retention	Personal information shall not be used or disclosed for the purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.
Accuracy	Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
Safeguards	Personal information shall be protected by security safeguards appropriate to the sensitivity of the information
Openness	An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
Individual Access	Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate
Challenging Compliance	An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance

4.2 Method

Several methods were used to collect the data from the various data sources, with each data source being analyzed for data relevant to the research question. Content analysis was used to extract the data from Maclean's magazine and the Reports of the Privacy Commissioner (questions one and two). A comparison of the privacy statements to the relevant principles in Canadian law was conducted to collect the data for the third research question.

In addition to the content analyses, descriptive data were also collected for two of the data sources. For the articles from Maclean's, article location (i.e., page number) and article length (i.e., word count) were collected; and for the privacy policies, the number of links (i.e., number of "mouse clicks" the user required to locate the privacy policy) to the privacy policy from the main page, the number of words in the policy, the reading ease, and the analogous grade level of the English were recorded. Reading ease refers to the Flesch reading ease and grade level refers to the Flesch-Kincaid grade level. These two measures determined the comprehension difficulty of a written work and were calculated using Microsoft Word.

4.2.1 Maclean's Magazine

For the first content analysis, the electronic vender EBSCOhost was used to search issues of Maclean's magazine for relevant articles. The filters on the vender were set to search for issues from January 1, 1992 to December 31, 2007, with different key words being used to identify relevant articles. *Relevant* was determined by searching for articles that began with the definition of internet privacy discussed earlier; for example, articles relating to the loss or threat to personal information, the social value of privacy, or secrecy on the internet. The search was further expanded to include related concepts such as databases or Big Brother to ensure all relevant articles were captured. A record of the different search terms used (e.g., computer privacy, internet privacy, or internet security) was kept. New search terms were input until no new articles were found, a "snowball" analysis technique. For each relevant article, the date, page number, word count, and author were recorded in a spreadsheet, and

an electronic copy and paper copy of the article were created. Each article was read twice: first, to determine whether it addressed the research question, and second to determine how it addressed the research question. Notes on the key issues presented in each article were collected in a spreadsheet. From these notes, the articles were grouped according to the similarities that were observed. The categories of similar articles were not determined before the analysis, but emerged as the articles were compared to each other. Finally, the articles, in chronological order, were compared to the timeline (Figure 3.1) to observe any differences between the technical development and the issues of privacy presented by Maclean's magazine.

4.2.2 Privacy Commissioner's Report to Parliament

A similar approach to that used for the analysis of Maclean's magazine was followed for the content analysis of the Privacy Commissioner's Report to Parliament and for the privacy policies. A copy of each annual Privacy Commissioner's Report from 1992 to 2007 was obtained from the Commissioner's website. In 2004, the Report to Parliament was separated into two documents, one reporting on the Privacy Act, the other, on PIPEDA. Both reports are included in this research. Each report was read and sections relating to the research question reflecting the criteria for internet privacy or the related discussion (e.g., databases) were highlighted. Notes on each section were recorded in a spreadsheet, and based on these notes, the discussions were grouped into emerging categories. Again, the discussions, in chronological order, were compared to the timeline (Figure 3.1) to observe any differences between the technical development and the issues of privacy presented by the Privacy Commissioner.

4.2.3 Privacy Policies

The top 100 most visited websites from the Alexa list of December 17, 2007 were identified. For each website, the web address, existence of a policy, date accessed, date of policy, and number of links to the policy from the homepage were recorded. Each policy was saved in HTML form (i.e., HyperText Markup Language or as seen on the actual

webpage) and copied into a Microsoft Word document. The grammar check on the Word document was run to determine the word count and comprehension difficulty of the policy. Then, each policy was examined using the measurement guide for the clauses of Schedule 1 in PIPEDA (Principles Set Out in The National Standard of Canada Entitled Model Code for The Protection of Personal Information, CAN/CSA-Q-830-96). Specifically, compliance to each sub-clause was recorded as either *Yes* (in compliance) or *No* (noncompliant). As well, additional notes regarding aspects of the policies relevant to the research questions were recorded on the spreadsheet.

Two content analyses, one of Maclean's magazine and the other of the Privacy Commissioner's Report to Parliament, and a compliance audit of popular websites are the source of data for this research. In the following chapter, the data gathered using these methods are reported.

CHAPTER 5: RESULTS

5.1 The Role of the Popular Press in Educating Canadians about Internet Privacy

One hundred and fourteen articles involving internet privacy were identified in Maclean's magazines. The analysis of the 114 pieces produced seven themes: (a) anonymity, (b) credit card security, (c) databases with personal information, (d) illegal access to computer systems, (e) legality, (f) malware or harmful software, and (g) security of computer systems. Six of the themes, credit card security, databases, illegal access, legality, malware, and security of systems, related directly to issues of deviance (or deviant activities) on the internet. An additional eighth category, *other,* was added for two articles that did not reflect one of the seven themes. Each article was classified as belonging to one of the six themes; that is, the articles were only coded once. A full description of the categories is found in the Table 5.1. In addition, Table 5.1 reports the number of articles found in each category and the year the first article appeared.

Table 5.1: Internet Privacy in Maclean's Magazine

Category	Types of articles	Total Number of articles	Year of first articles
Database	electronic files containing information about groups or individuals	12	1992
Malware	malicious software (i.e., viruses) that poses a privacy risk	14	1992
Credit Card	privacy issues related to use of credit cards online (i.e., scams)	6	1994
Legal	legal issues (i.e., cases or laws) that relate to internet privacy	15	1994
Security	physical risks (i.e., unsecured laptop) that threatens privacy	29	1994
Hack	illegal or unauthorized access to electronic files containing personal information	22	1995
Anonymity	issues of maintaining personal anonymity while online	14	1996
Other	any internet privacy article that does not fit into the previous seven categories	2	1999

Table 5.1 indicates that the most prevalent types of internet privacy articles in Maclean's were those concerning security (29 articles, or 25%) and hacking (22 articles, or 19%). Security articles were most prevalent in 2006 and 2007 (6 articles, respectively, or 41%). The largest number of articles related to hacking appeared in 2000 (7 articles, or 32%). The least prevalent type of article was credit card fraud (6 articles, respectively, or 5%).

Of the 114 articles, the largest number for one year appeared in 2000 (17 articles, or 15%); the least, in 1992, 1993, and 2002 (2 articles for each of the three years, respectively; see Figure 3). There were 38 articles relating to internet privacy before 2000 (1992-1999) and 59 after 2000 (2001-2007).

Figure 5.1: Internet Privacy in Maclean's Magazine by Year

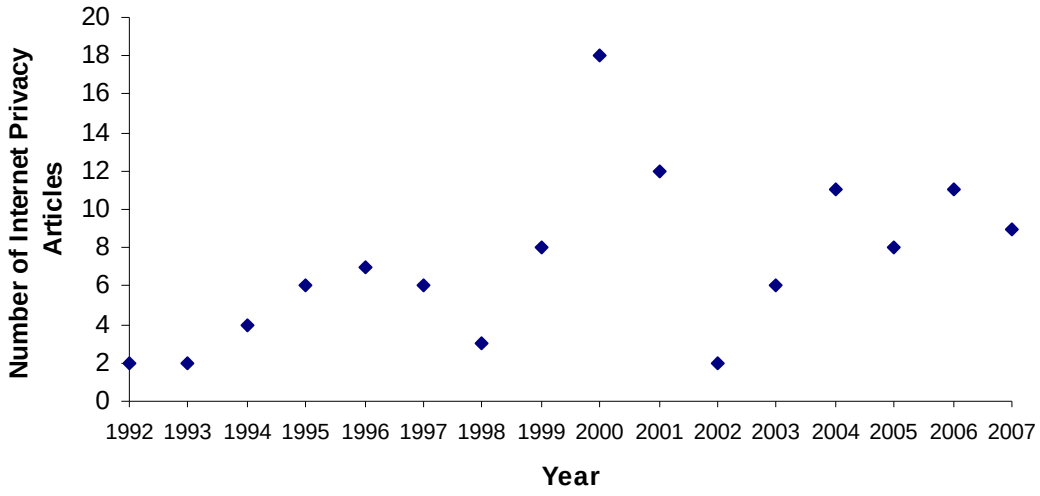


Figure 5.1 shows four peak years for the internet privacy articles: 1996, 2000, 2004 and 2006. The first peak corresponds to the increasing financial success of the internet, the "dot com bubble"[4] of the mid 1990s; the second, to fears surrounding Y2K[5] and the "dot com bust" of 2000, specifically, the privacy issues concerning increased business on the internet (e.g., collecting and protecting personal information). The fourth peak corresponds to the increasing concerns surrounding the use of social networking sites such as Facebook or MySpace, reflecting the increased amount of personal information posted on social networking sites. And the third peak in 2004 does not appear to correlate with any particular internet related event. Further, when compared to the Timeline (Figure 3.1), the

[4] With the increase in technology companies during the late 1990s, the value of Western markets increased. The "bubble" burst in 2000, perhaps due to Microsoft losing an American court battle concerning the company's monopoly on operating systems.

[5] Y2K (Year 2000) refers to a concern that computer systems would fail when the date changed from 1999 to 2000. Many computer programs only recorded the year with two values (e.g., 96, 97, 98) and some systems were not able to start "recounting" (e.g., 00, 01) on January 1, 2000.

Maclean's articles did not reflect the privacy issues associated with the advancing technology, indicating a bias in the Maclean's reports. That is, trends in the Maclean's articles relating to internet privacy did not reflect the trends in technological development.

For the 114 articles, the mean length was 938 words, with a mode of 1186, a median of 838, and a range of 4954 (48 to 5002) words. Nine Maclean's articles concerning internet privacy were also cover stories: two cover stories in 1995, two in 1996, one in 1998, one in 1999, two in 2001, and one in 2006. The cover stories appeared in the magazine coincidental with the peaks in Figure 3.1. The 1996 cover stories addressed the risk to business of hackers and the amount of information available on the internet; the 1998 cover story addressed data-mining; and, the 1999 cover story, internet pirates. These four cover stories related to issues of business on the internet during the dot com bubble and subsequent burst (the first two peaks on Figure 3.1). The 2001 cover stories addressed spying and the general security concerns that emerged in the early 21st century (prior to peak 3). The 2006 cover story addressed increasing discussion of social networking sites (peak 4).

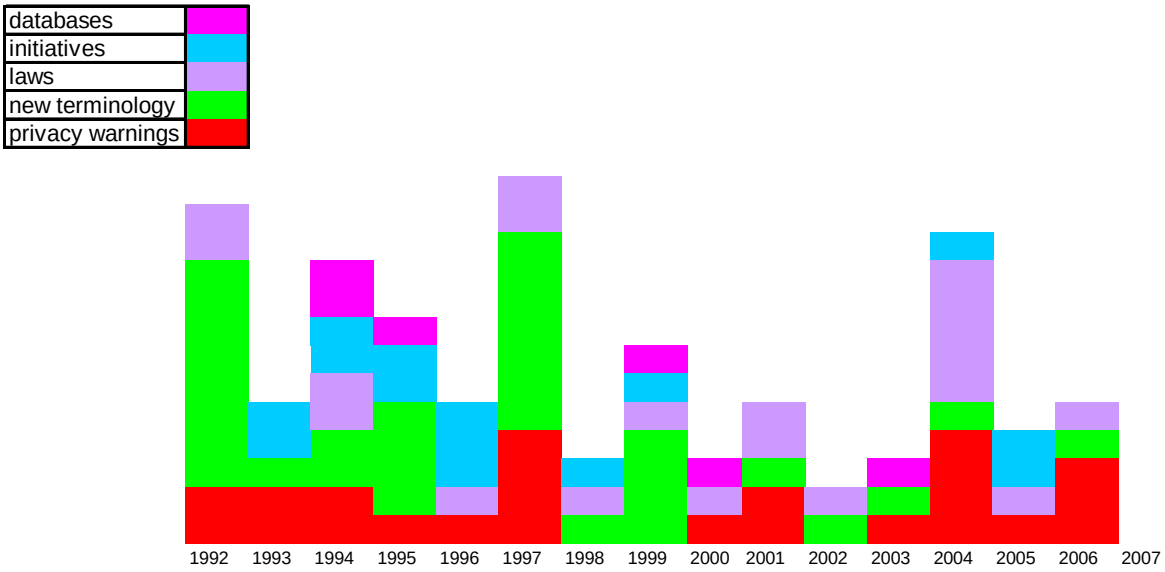
5.2 Political Response to Internet Privacy Concerns

The results of the discourse analysis on the Privacy Commissioner's Report to Parliament generated five themes concerning internet privacy: (a) the impact of electronic databases on internet privacy (b) internet privacy initiatives, (c) legislation relating to internet privacy, (d) the impact of new technology and the resulting new terminology on internet privacy discussions and (e) privacy warnings. A full description of the categories appears in Table 5.2. The table shows the number of discussions found in each category and the year the first discussion appeared. Figure 5.2 shows the number of discussions per category by year.

Table 5.2: Internet Privacy in the Privacy Commissioner's Reports

Category	Types of discussion included	Total number of references	Year first appeared
Law	legislation or policies relating to internet privacy	19	1992
privacy warnings	shortcomings of Privacy Act or PIPEDA to protect personal information	24	1992
new terminology	first use of technical terms or jargon	32	1992
Initiatives	surveys, plans, commitments, or calls for legislation relating to internet privacy (ties closely with *law*)	14	1993
Database	information stored in electronic databases and the use of the database	6	1994

Figure 5.2: Internet Privacy in the Privacy Commissioner's Reports by Year



These results indicate that issues concerning personal privacy on the internet were a topic of concern for the Privacy Commissioner in 1992, the first year analyzed for this research. In 1992, the Commissioner acknowledged that information was routinely exchanged over electronic databases, and that the emerging technology would threaten individual control over personal information. In 1993, the limitations of the Privacy Act (1983) with respect to technology were discussed, and the Privacy Commissioner called for new privacy legislation. However, the Commissioner did acknowledge that legal interpretations of the

existing Act had been used in cases involving privacy and technology. An additional limitation of the Act noted by the Privacy Commissioner was that the Act did not cover all government departments or businesses in Canada.

In 1994, the Privacy Commissioner's concern shifted to business activities and databases on the internet; specifically, the Commissioner was interested in personal information that was valuable to businesses and government. For example, a controversial policy in effect between 1994 and 1996 which allowed Customs data to be matched with Employment Insurance (EI) data in order to identify EI abuse represented a type of data aggregation the Privacy Commissioner thought violated the Privacy Act. In 1995, the Commissioner argued that no computer was safe from hackers. In 1996, the federal government committed to new privacy legislation governing personal information and business, legislation that reflected the changing technical landscape. In 1997, the Commissioner warned that Canadians were relying on systems that were not secure. The Commissioner's concerns were addressed when Bill C-54 (PIPEDA) was tabled in 1998, passed the House and Senate in 1999, and became law in two phases, beginning in 2001 and ending in 2002.

In 2001, the Commissioner warned against using the events of September 11, 2001 terrorist attacks on the United States[6] as a "Trojan horse" to acquire invasive power at the expense of the privacy acts. Later, in 2005, the Commissioner argued that the Privacy Act had been weakened by the Anti-Terrorism Act of 2001[7].

With respect to internet privacy, the results of this analysis of the Privacy Commissioner's Reports indicate the focus of the federal government has been to create legislation to protect data concerning Canadians stored within Canada and to regulate the transfer of data. When

[6] An Islamic terrorist group hijacked four jetliners on September 11, 2001. Two were flown into the World Trade Centre buildings in New York City, and one into the Pentagon (Headquarters of American Department of Defence). The remaining aircraft crashed into a field in Pennsylvania before it could reach its target

[7] Some of the controversial clauses in the Act were sunset in 2007 and were not renewed by a House vote in February of that year

the results were compared to the Timeline (Figure 3.1), it appears that the Privacy Commissioner was considering the implications of the new technology with respect to the privacy of Canadians. For example, in 1997, the Privacy Commissioner was considering the impact of cryptology (encrypting data transferred on the internet). Similar discussions were also being considered in the United States, eventually leading to the relaxation of the rules on cryptology "keys" in 2000.

5.3 Privacy Protection on Commercial Websites

The final data source examined was the privacy policies of the 100 most visited website sites by Canadians. Of the 77 useable (i.e., English, non-pornographic) websites, eight had no privacy policy, or the link to the privacy statement was inoperative. Of the 69 websites with privacy statements, seven could not be used: one claimed not to collect any information, two did not collect any information, two did not indicate if personal information was collected or not, and the other two had privacy policies that only applied to American citizens. Although only 62 websites were included, in all, 63 privacy polices were analyzed because one site had two policies (2 parent companies with different policies).

As mentioned earlier, each of the clauses subsumed under the ten principles of Schedule 1 was operationally defined based on *internet privacy*, and then the compliance to the clauses was assessed for each privacy statement. In the tables below the measure of each clause is described, and the percent compliance (i.e., percentage of the privacy policies which complied with the clause) is indicated. Ten sub-clauses were omitted from the analysis because they were not relevant to the internet environment or were undeterminable. For example, clause 4.4.2 "consent with respect to collection [of personal information] is not obtained through deception" cannot be determined by reading the privacy policy; that is, if the owners of a company operating a website are deceitful, the privacy policy is unlikely to indicate the deception. Table 5.6 (presented later) summarizes the results of sub-clause 4.3.2., compliance, indicating if companies complied with "reasonable" effort and "meaningful" consent the location and reading difficulty of the policies.

Table 5.3 shows that the first principle, accountability, had 57% compliance. (Overall compliance was measured as the average compliance for each of the sub-clauses.) The name of the Privacy officer was not usually provided (41%), but the address or email address of that individual, or the contact information, was (77%). However, there was little indication the privacy policies of the companies were communicated to the staff. Most of the organizations took responsibility for the security of personal information that they had collected, but this responsibility only extended to other businesses hired to fulfil the services of the organization. That is, responsibility did not extend to third parties that also operated on the websites, for example, advertisers. Often, the privacy polices indicated that the third parties had their own privacy policies, policies that might not provide the same level of protection for personal information.

Table 5.3: Schedule 1, Principle 1

Principle	Measure	Percent compliance	Overall
Accountability			**57%**
4.1.1	name of Privacy Officer (or equivalent)	41%	
4.1.2	name of person who oversees compliance available by request	77%	
4.1.3a	organization accepts responsibility for safe-keeping of personal info;	83%	
4.1.3b	equivalent protection data transferred to 3rd parties guaranteed	40%	
4.1.4a	procedure to protect personal info. Stated	84%	
4.1.4b1	mechanism to make a complaint (regarding personal info.) included;	73%	
4.1.4b2	guarantee of response	9%	
4.1.4c	privacy policies are communicated with staff	10%	
4.1.4d	(electronic) privacy policy or privacy procedure	93%	

The second principle, identifying purposes, examined how the purposes for the personal information were communicated to the users. While the overall compliance rate for this category was 61%, two sub-clauses (4.2.3 and 4.2.4) explaining how information is used

(e.g., marketing) had 70% and 89% compliance. Of particular interest was the PIPEDA clause (4.2.2) -- that only necessary information was collected. In many cases, the policy stated that the purpose of some of the information was for advertising purposes, meaning the information was required specifically for advertising purposes and not necessarily required for the service the organization was providing for the user.

Table 5.4: Schedule 1, Principle 2

Principle	Measure	Percent compliance	Overall
Identifying Purposes			**61%**
4.2.1	organization has a privacy policy beyond the electronic public version	3%	
4.2.2	only necessary info. collected (compare to the purpose)	81%	
4.2.3	purpose for collection of personal info. stated before/time of collection	89%	
4.2.4	states that consent for additional uses of personal info. collected before use	70%	

The third principle, consent, had 54% compliance. However, one important sub-clause -- that consent be obtained prior to use -- had an 81% compliance rate. Most of the policies indicated how consent would be obtained, but often the consent was negative. That is, by conducting business using the site, users accepted the organization's privacy policy regardless of whether the policy was actually read by the user. Further, only a little over half (56%) of the companies provided a procedure for withdrawing consent.

Table 5.5: Schedule 1, Principle 3

Principle	Measure	Percent compliance	Overall
Consent			**54%**
4.3.1	consent obtained for collection and use of personal info.	81%	
4.3.2	"reasonable" effort; "meaningful" consent	see Table 5.6	
4.3.3	are there any mandatory fields that would prevent obtaining the product beyond necessary for stated purpose?	0%	
4.3.4	is the information collected "sensitive" (i.e., reasonable need for privacy?)	77%	
4.3.5	statement of additional anticipated purposes for the personal info. Collected	77%	
4.3.6	consent for information "like to be considered sensitive" obtained?	79%	
4.3.7a	online form?	71%	
4.3.7b	checkbox?	0%	
4.3.7c	telephone?	6%	
4.3.7d	at use of product/service?	43%	
4.3.8	mechanism for withdrawing consent stated	56%	

Sub-clause 4.3.2 stipulates that access to details regarding what data will be collected should be reasonable to obtain, and the consent to data collection should be meaningful to the user. "Reasonable" was interpreted to mean (a) the ability to find the policy, measured by number of links (or "mouse clicks") to the policy from the homepage; and (b) "meaningful" consent, to the length of the privacy statement, reading ease, and grade level, based on the Flesch-Kincaid reading ease test. Table 5.6 shows the average policy had a word count of 2200 words, or approximately nine pages double spaced, had a reading ease of 33, and a grade level of 12. The longer policies were more specific in their levels of protection, but more reading was required from the user to ascertain the protection. The reading ease score was calculated based on the total words, sentences, and syllables in a piece of text. Reading ease is measured on a 100 point scale: 0-30 (very difficult), 31-50 (difficult), 51-60 (fairly difficult), 61-70 (standard), 71-80 (fairly easy), 81-90 (easy), and 91-100 (very easy). For comparison, Reader's Digest articles usually score 65 (Kerr, 2007). As the above point-scale indicates a reading ease of 33 indicates that the privacy policies were "difficult" to understand, a comparable reading level to a *Harvard Law Review* article

(Kerr, 2007). This writing standard was observed for many of the privacy statements, which were often written in a legalistic manner. The grade level,12, indicates the equivalent (American) school level.

Table 5.6: Schedule 1, Principle 3, Sub-Clause 4.3.2

	Average
Number of clicks	1.3
Word Count	2192
Reading Ease Score	32.6
Grade	12.13

The fourth principle, limiting collection, is related to the third principle in that the request for personal information matches the purpose of the service offered by the organization. Again, if the purpose was to gain information for advertisers then this purpose was relayed to the user. Advertising in this manner is unique to the internet, for it is impossible to use most websites without providing identifying information, whereas in non-internet interactions, the customer is not always required to provide identifying information (e.g., paying for purchases with cash). Many of the organizations collected environment data (e.g., entry/exit page, IP address, CPU, and browser information), some of it personal in nature, from all users who visited the site, regardless of whether the user actually selected any of the services available on the site. Although environmental data may not be considered personal information, the IP address, for example, can identify a specific user's computer.

Table 5.7: Schedule 1, Principle 4

Principle	Measure	Percent compliance	Overall
Limiting Collection			**83%**
4.4.1	personal info. collected matches purpose	83%	

The fifth principle concerned the retention time of personal information. None of the policies required that personal information be destroyed after a set period of time. However, for the policies that did address retention times, the interval was addressed in three ways: “indefinitely”, until “no longer required”, or “as required by law”. Although 17% addressed retention times, none gave a specific timeframe for destruction of information.

Table 5.8: Schedule 1, Principle 5

Principle	Measure	Percent compliance	Overall
Limiting Use, Disclosure, and Retention			**9%**
4.5.2	states retention times for personal info.	17%	
4.5.3	states when personal info. is destroyed; organizational policy states when personal info. is destroyed	0%	

The sixth principle, accuracy, addressed whether there was a system to update the information. Sixty-six percent of the organizations had methods for updating users personal information, but most were user dependant. That is, often the personal information was updated by the user – the user accessed his/her account on the website and made the required changes.

Table 5.9: Schedule 1, Principle 6

Principle	Measure	Percent compliance	Overall
Accuracy			**23%**
4.6.1	procedure in place to insure accuracy, completeness, and up-to-datedness of info.	66%	

4.6.2	info. is not routinely updated unless required to fulfill original purpose	0%	
4.6.3	info sent to third parties is updated; how?	3%	

The seventh principle, safeguards, addressed the protection of personal information stored by organizations. Seventy percent of organizations stated that they protected the information, but most did not indicate how this was accomplished. That is, they did not indicate what form of protection was used -- physical, organizational, or electronic. Determining if the level of protection matched the sensitivity of the data was, of course, subjective, but if the organization mentioned at least one method of protection, then the level was assumed to be sufficient.

Table 5.10: Schedule 1, Principle 7

Principle	Measure	Percent compliance	Overall
Safeguards			**28%**
4.7.1	states that personal information is protected by specific safeguards	70%	
4.7.2	is protection (4.7.1) consistent with sensitivity of info (4.3.4)?	40%	
4.7.3a	statement of physical protection measures?	10%	
4.7.3b	statement of organizational measures?	27%	
4.7.3c	statement of electronic measures?	36%	
4.7.4	organizational policy is communicated to staff	13%	
4.7.5	statement to the provisions to protect personal info. when it is being destroyed	0%	

The eighth principle, openness, addressed the types of information that were collected. Most of the organizations stated the type of information collected (74%), but not what information was passed to third parties (26%).

Table 5.11: Schedule 1, Principle 8

Principle	Measure	Percent compliance	Overall
Openness			**49%**

4.8.1	policy is available online ("reasonable" effort for web based organizations)	94%	
4.8.2c	description of personal info. held	74%	
4.8.2e	description of what personal info. is released to related organizations	26%	
4.8.3	privacy policy available in other (non-electronic) forms	1%	

The ninth principle, individual access, had a compliance of 23%. Most organizations corrected inaccuracies in their data but did not give a timeframe, price, or procedure for dealing with unresolved complaints. Twenty-nine percent of organizations provided a list of the third parties that received personal information, but except for one case, the list did not include organizational names, just types. That is, rather than giving specific company names (e.g., Oracle or Microsoft), the third parties were only identified by their association to the organization (e.g., affiliates, sister organizations, or parent companies). This anonymity makes it difficult or impossible to know the level of privacy protection extended by the third parties.

Table 5.12: Schedule 1, Principle 9

Principle	Measure	Percent compliance	Overall
Individual Access			**23%**
4.9.2	states information required to access personal info. accounts	7%	
4.9.3	list of possible third parties who receive info.	29%	
4.9.4	time frame for requests stated; cost of request stated; form of info. stated	4%	
4.9.5	organization mends inaccuracies	64%	
4.9.6	procedure for dealing with unresolved complaints stated	11%	

The final principle, challenging compliance, addressed how to make a complaint. Eighty-one percent of the organizations had an easily comprehended method for complaining (e.g. email address to send enquires), but only one organization guaranteed an investigation.

Table 5.13: Schedule 1, Principle 10

Principle	Measure	Percent compliance	Overall
Challenging Compliance			**55%**
4.10.2	procedure for complaining is "accessible" and "simple"	81%	
4.10.3	procedure for dealing with complaints stated	81%	
4.10.4	assurances of investigation of complaints given; assurance that changes made if complaint valid	1%	

With respect to internet privacy, the privacy policies in general do not reflect the clauses of Schedule 1. Certain clauses (e.g., 4.1.4b, mechanism to make a complaint included) had fairly high compliance rates; whereas, other clauses within the same principle (e.g., 4.1.4c) had very low compliance rates.

In summary, Maclean's magazine had 114 articles over the fifteen year period focusing primarily on the lack of security on the internet. The number of articles was found to track current events. The major achievement of the Privacy Commissioners was the introduction of Canada's electronic document act. The evaluation of the 100 websites revealed significant non-compliance with Canada's electronic document act. In other words, most of the clauses in PIPEDA were not supported by the privacy policies posted on the websites.

CHAPTER 6: DISCUSSION

6.1 Discussion of the Three Research Questions

The first research question, *How has the popular press educated Canadians about the potential changes in personal privacy associated with the advances in technology?*, was considered from the perspective of Maclean's magazine. Often the news media are the primary source of information for Canadians regarding issues of public affairs, and media, such as Maclean's, are responsible for "setting the agenda" with respect to news (McCombs, 2004). The results of this research indicate that Maclean's writers focused on the threats to internet privacy. Their articles examined the sensational aspects of internet privacy issues, such as the impact of viruses (e.g., the damage caused to computers by the *LoveBug* virus) and the criminal uses of the internet (e.g., the "Denial of Service" attack by the Canadian teen *MafiaBoy*, who inundated a server with requests, causing the system to crash). By focusing on the deviant uses of the technology, Maclean's writers left unexamined the underlying structure of the internet system, a structure which made the deviance possible.

Of particular interest was the uneven coverage of privacy issues: there were four peak years, with the number of articles levelling off between the peaks. The results showed that the peaks were roughly linked to specific events of importance in Canadian current affairs, such as the commercial dot com boom of the 1990s. By focusing on specific privacy events, the continual changes in the internet that influence privacy were not addressed by Maclean's writers, perhaps leaving the impression with readers that privacy issues are isolated events.

The second research question, *What has been the political response from the Canadian federal government to the potential changes in personal privacy associated with the advances in technology?*, addressed the political response to internet privacy concerns. The Privacy Commissioner reported on two aspects of internet privacy: (a) the legislative

process to introduce new electronic privacy law, and (b) the privacy issues that would need to be considered by Canadians. The Commissioner continually addressed these two issues every year in the context of the current events. For example, in 2000 and 2004 the Commissioner warned about the impact of anti-terrorism legislation, a warning which corresponded to the increase in privacy articles in Maclean's magazine. Given the international nature of the internet, national-level responses (such as PIPEDA) to internet privacy issues are not likely to be enough to protect Canadians. However, from this research, it is apparent that the Commissioners' were *raising the flag* for Canadians. That is, they were alerting Canadians of the threats to internet privacy.

The third research question, *Do the privacy statements on the most popular commercial websites accessed by Canadians protect their personal information?*, addressed the commercial uses for personal information and the threat to internet privacy. The findings suggest that most of the business websites contained privacy policies that were in keeping with only some of the provisions of PIPEDA, and the policies were not always that specific about the mechanisms for protecting personal information. It is a concern that many policies indicated the collection of personal information for marketing purposes was part of the company's business plan. Such uses can be interpreted as a violation of PIPEDA as the information was being acquired for purposes not related to customers' purchases. Disturbingly, as noted by Hui, Teo, and Lee, users will supply more personal information if a business posts a privacy policy, but as this research indicates, the privacy policies are not specific enough to suggest adequate coverage (2007).

Commercial businesses obtain personal details during user registration for online services (e.g., email from Hotmail) or the purchase of products (e.g., books from Amazon). The results of this research suggest that for the users, once their personal information has been obtained, knowing how or where this information is stored, who will be given access to it, how the information will be used, and knowing whether it will be combined with other personal details for purposes unrelated to the initial transaction is difficult to ascertain. From the results, (specifically, Principle 3 and sub-clause 4.3.2) it is clear that the privacy statements are not easy to read, a finding which does not reflect the PIPEDA requirement

for the policies being accessible and user consent meaningful. In other words, these policies are challenging to read (i.e., a "difficult" reading rating) and comprehend (i.e., a grade "12" comprehension level), which makes meaningful consent difficult to assess. This issue is further compounded since the more complex privacy policies were more likely to address more of the privacy clauses, but the policies were longer and more challenging to read. Further, these results are supported by the research of Graber, D'Alessandro, and Johnson-West who also found privacy policies to be difficult to read (2002). It appears then that the collection of personal information "results in little or no choice for Internet users and relatively few meaningful privacy mechanisms" (Privacy International, 2007).

6.2 Understanding Internet Privacy using CAS Theory

A complete understanding of internet privacy cannot be achieved from any one of the agent's perspectives discussed above. However, Complex Adaptive Systems theory provides a more holistic approach to internet privacy by integrating the different perspectives. Specifically, there are four elements of CAS that can guide an explanation of internet privacy: co-evolution, fitness landscapes, path dependency, and waves (Walby, 2005).

Co-evolution is an alternative way of conceptualizing change within complex systems. That is, in systems like the internet that lack a centralized mechanism of control, change, instead of being hierarchical and reactionary, is a transforming process, achieved through the interaction of different agents and the environment. The agents' responses to privacy evolve as they adapt to their environment; their responses do not reflect the pressures inherent in a hierarchical system. In other words, changes to internet privacy cannot be imposed on the system from any one agent. When the federal government enacted legislation (i.e., PIPEDA) to control internet privacy, it was a response from a traditionally hierarchical system and unlikely to be successful on the internet. For instance, the privacy policies of the businesses, which would be expected to reflect current law in a hierarchical system, did not on the internet.

Each of the agents operating on the internet influences the limits of privacy – when one agent changes, the internet environment changes, and therefore, the other agents are impacted (Walby, 2005:1). Accordingly, when government introduces legislation to protect privacy, users are educated about the security risks to privacy, and businesses produce privacy policies to secure the collection of information; then, the overall environment becomes one of system security. In other words, the internet is *autopoiesic*, where "each component participates in the production or transformation of other components in the network" (Walby, 2005:13). For example, in the beginning of commercial activities on the internet, a credit card purchase only required the name, number and expiry date as the actual card cannot be offered in the transaction. This use of card numbers has led to widespread internet credit card fraud, and in an environment of system security, a litany of secondary passwords are now required from legitimate card-holders. The Bank of Montreal, for instance, often requires not only name, credit card number, expiry date, but additional passwords or questions, with answers known only to the legitimate card-holder, to allow certain internet purchases. The interaction between agents creates the environment, or the structure, of privacy – a structure dominated by security as opposed to protection of privacy.

The internet environment, where the different agents interact causing change, can be considered as a *fitness landscape* (Walby, 2005:2). That is, as the internet develops through interactions, its changing environment is more suited to some types of changes than others. The most prevalent changes observed in this research were technical: the changes in business and government were transforming as the technology changed. For example, the technology to create and "mine" databases was in place before government, business, or users realized its possible applications. As the interactions between agents changed and the applicability of the technology emerged (e.g., enough users on the system to warrant commercial databases), the environment changed.

Path dependant change suggest that (a) events impact the system at a later point (i.e., history matters), and (b) the order in which such events occur may also impact system change. Paths can cause sudden system changes or gradual changes (Walby 2005:2,15). Path dependence does not contradict the earlier discussion of chaotic system (e.g., no

repeating patterns of change or states of equilibrium); that is, path dependence does not imply *linear* change, only that historical events may influence current events. For example, data storage devices in the early 1990s were disks with increasingly large memory space, but with the introduction of USB storage devices, disks quickly fell out of general use. An interesting example for application of path dependency is seen when social and political institutions often "lock in" on particular path developments based on their "power, opportunity and knowledge" (Walby, 2005:15). Such a "lock in" exists for as long as that particular path is impacting the system. This study found that the federal government has "locked in" on internet regulation as its approach to protecting privacy. That is, when the Privacy Commissioner called for legislation in 1993, the focus of the federal government was and has been on enacting privacy legislation to regulate electronic information.

Earlier in this thesis, privacy was conceptualized using the metaphors (*Big Brother* and *The Trial*); one final metaphor that CAS theorists use to conceptualize the change in a system is the term *wave* (Walby, 2005). The wave is a conceptualization of the non-linearity of systems like the internet; it is the "simultaneous temporal and spatial dimension of [non-linear] social change" (Walby,2005:16). The wave starts in one location, then builds and spreads through space and time affecting other agents in other locations, depending on the local conditions. The changes are connected, not linearly, but through the networks linking the agents. The wave is not an institution; rather, it is the energy of transformative change that passes through the different agents operating in a system. Internet privacy can be conceptualized as a wave that is affecting all the agents operating on the system through their interactions (or networks). This wave started when the internet opened to general users in the early 1990s, and it has affected how businesses operate, how government regulates, and how users interact, creating a system where privacy is impossible to maintain.

6.3 Conclusions

This research has demonstrated that it could be argued the evolution of the internet has created an environment where privacy cannot exist. Every user, every web page visited, and every key stroke is captured electronically, often unbeknownst to the user. The unprecedented amounts of personal information users willing share with web masters has

led to the development of new goods and services that further reduce their privacy. For example, using its database of purchase histories, Amazon (an internet-based bookstore) emails its customers to announce the publication of a new book by their favourite author. The internet is not controlled centrally and individual countries can do little to adequately protect their citizens. Certainly, given the low compliance rate with PIPEDA suggested by this research, it is clear that Canadian federal laws are not protecting Canadian online users. Further, users are not being educated about how their personal information is being collected and used for commercial purposes; instead, they are being informed of the criminal or deviant aspects of privacy loss.

In summary, users exchange information to complete commercial transactions. Embedded in the transactions are a number of additional personal data elements (e.g., businesses collecting additional personal information for advertising which is not required for the original transaction) that are not only reusable, but are also a form of currency that can be exchanged with others for purposes unrelated to the initial exchange. Governments have an interest in controlling or monitoring these interactions, although the system is beyond national level control. It is clear that the control of internet privacy does not belong to any of the agents; that is, users are unaware of the structural limits to privacy, government cannot produce effective laws to protect privacy, and business are capitalizing on the opportunities that advances in the technology are creating (e.g., data-mining software). It would appear that technology creates the wave that agents respond to, suggesting that privacy will continue to erode. In other words, technology usurps the privacy afforded in traditional agent interactions.

This study has shown that the internet is a complex system, with structural barriers originating in agent interactions that limit internet privacy. Further, educational sources such as Maclean's magazine that could raise awareness of these structural limitations, do not, but the Privacy Commissioners have made Canadians aware of specific threats to personal privacy emerging from internet development and the extent of their legal protection. However, Canadian legislation (PIPEDA) controlling the use of personal information in electronic forms is not effective in regulating the websites of Canadian's

most visited sites. This research has shown the inability of the user or government to control the movement of personal information throughout the system. The system operates internationally, making it difficult to know precisely where information is stored. In addition, where the servers (with databases of personal information) are located, and what policies and procedures apply to the storage, retrieval, and use of the information (e.g., physical or organizational) is difficult to know or change. Data do not travel in a direct path from source to destination; rather, data travel through multiple systems (e.g., routers), systems which present numerous structural opportunities for interception.

This research report began with a decade old quote regarding privacy on the internet; namely, "[we] have zero privacy anyways". The results of this research suggest the comment would appear to be accurate: (a) national level governance is not enough to protect Canadians, and international governance is not yet in place, (b) business has commodified personal information for commercial purposes, and (c) a major Canadian magazine does not educate Canadians regarding how structure influences internet privacy. The internet is a dynamic system which needs a systematic privacy initiative to ensure that privacy, one of Canada's social values, is not undermined further. Such an initiative likely needs to incorporate an increased user awareness of the limitations of privacy on the internet and the consequences to society from the loss. Further, it is unlikely that a traditional hierarchical system of control, such as an international regulatory body, will successfully reverse the loss of privacy. Perhaps, increasing the transparency of the system will allow users to influence privacy protection.

6.4 Research Limitations

There are two limitations to this research: (a) compliance with the terms in the privacy policies, and (b) Maclean's bias. First, there is no supporting evidence that any of the businesses whose privacy policies were analyzed are actually in compliance with their privacy provisions. That is, the actions of the businesses in relation to privacy were not assessed. Auditing companies operating on the internet may be the most reliable method of addressing compliance. Second, the potential bias in Maclean's magazine from the writers/publishers is reflected in the magazine's focus on deviance on the internet.

Examining other media sources, for example newspaper, radio, and television, would address this limitation.

6.5 Future Research

Two aspects of internet privacy which could lead to future research are the following: (a) the international regulation of the internet, and (b) the increasing interest in social networking sites. First, different nations have different requirements regarding privacy, different interpretations of what privacy means, and different motivations for creating privacy standards (Wafa, 2008). These three aspects would all need to be considered when attempting to regulate the internet. Such international cooperation regarding the internet is possible; for example, the European Union (EU) has a shared standard of privacy protection covering all member countries. Part of the impetus for Canada's new privacy law was the EU requirements that all data transferred out of the EU be protected by similar measures followed in the EU (Knight, Chilcott & McNaught, 2006). It is, however, difficult to evaluate the effectiveness of the EU guidelines as a form of international regulation. For example, the EU and the United States formed a *Safe Harbour* agreement, which aligned American companies with the EU guidelines. But in the nine years *Safe Harbour*s has operated, none of the 1300 American participants has ever had its certification suspended or revoked (Wafa, 2008). Second, one of the latest trends on the internet is the proliferation of social networking sites such as Facebook or MySpace. These sites raise a number of privacy issues: for example, (a) the type of information users post, (b) the personal risks associated with posting (e.g., bullying comments), (c) the controls on the users who visit the postings, (d) the security of the system, and (e) the advertising potential. These sites are considered a “goldmine” to advertisers because of the user behavioural information that is available for commercial analysis (Wafa, 2008:12).

6.6 Final Word

This study has shown that Canadians should consider their privacy in this amazing time of technological development on the internet. The following quote, in tribute to George Orwell and Franz Kafka, serves as a warning: "Privacy is like health, when you have it, you don't notice it. Only when it's gone do you wish you'd done more to protect it."[8] (Wafa, 2008:15)

[8] Original quote is from Bob Sullivan, MSNBC, "Privacy Lost: EU, U.S. Laws differ Greatly" (Oct. 19, 2006)

REFERENCES

Bannister, Frank 2005. The panoptic state: Privacy, surveillance and the balance of risk. *Information Policy* 10: 65-78.

Beekman, George, Michael Quinn & Susan Anderson-Freed. 2006. *Computer Confluence*. Toronto, ON: Pearson Custom Publishing.

Bryman, Alan & James Teevan. 2005. *Social Research Methods*, Canadian Edition. Don Mills ON: Oxford University Press

Canadian Broadcasting Corporation. 2007. *Google Street View May Be Illegal: Canada*. Available at: http://www.cbc.ca/technology/story/2007/09/11/streetview-commissioner-privacy.html (Retrieved September 12, 2007).

Canadian Broadcasting Corporation. 2009. *Privacy Advocates concerned about potential internet wiretapping law*. Available at: http://www.cbc.ca/technology/story/2009/02/12/privacy-wiretap.html (Retrieved March 2, 2009).

Castells, Manuel. 2000. Toward a Sociology of the Network Society. *Contemporary Sociology* 29(5): 693-699.

Clapham, Andrew. 2007. *Human Rights, A Very Short Introduction*. New York, NY: Oxford University Press

Culnan, Mary, & Pamela Armstrong 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organizational Science* 10(1): 104-115.

Diffie, Whitfield, & Susan Landau. 2008. Brave New World of Wiretapping. *Scientific American*. September: 57-63.

DiMaggio, Paul, Eszter Hargittai, W. Russell Neuman, & John Robinson. 2001. Social Implications of the Internet. *Annual Review of Sociology* 27: 307-336.

Emirbayer, Mustafa. 1997. Manifesto for a Relational Sociology. *The American Journal of Sociology* 103(2): 281-317.

Foley, Jayni. 2007. Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases. *Berkeley Technology Law Journal* 22:447-475.

Graber, Mark, Donna D'Alessandro, & Jill Johnson-West. 2002. Reading level of privacy policies on Internet health Web sites. *The Journal of Family Practice* 51(7): 642-647.

Hinduja, Sameer. 2004. Theory and Policy in Online Privacy. *Knowledge, Technology, & Policy* 17(1): 38-58.

Holton, Robert. 2006. Talcott Parsons: Conservative Apologist or Irreplaceable Icon. In *Handbook of Social Theory*, editors, George Ritzer & Barry Smart. London, England: SAGE Publications.

Howe, Christina. 2002. *Book Review – The Laws of the Web: Patterns in the Ecology of Information*. Available at: http://www.ibm.com/developerworks/rational/library/2808.html (Retrieved December 4, 2008).

Hui, Kai-Lung, Hock Hai Teo, & Sang-Yong Tom Lee. 2007. The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly* 31(1): 19-33.

Internet World Stats. 2008. *World Internet Usage Statistics*. Available at: www.worldinternetstats.com (Retrieved October 19, 2008).

Kerr, D. 2007. Information in diabetes care: is there a need to dumb down even more? *Diabetic Medicine* 24(5): 561-563.

Knight, Jamie, Sharon Chilcott & Melanie McNaught. 2006. *Canada Personal Information Protection and Electronic Documents Act: Quick Reference*. Toronto ON: Thompson.

Larose, Daniel. 2005. *Discovering Knowledge in Data: An introduction to Data Mining*. John Wiley & Sons.

Lauer, Thomas & Xiaodong Deng. 2007. Building online trust through privacy practices. *International Journal of Information Security* 6:323-331.

McCombs, Maxwell. 2004. *The Agenda-Setting Role of the Mass Media in the Shaping of Public Opinion*. University of Texas.

Milne, George & Mary Culnan. 2002. Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal analysis of the 1998-2001 U.S. Web Surveys. *The Information Society* 18: 345-359.

Miyazaki, Anthony & Ana Fernandez. 2001. Consumer Perceptions of Privacy and Security Risks for Online Shopping. *The Journal of Consumer Affairs* 35(1): 27-45.

Office of the Privacy Commissioner of Canada. 2007. *Mandate and Mission of the OPC*. Available at: www.privcom.gc.ca/aboutUs/index_e.asp (Retrieved November 14, 2007).

Paine, Carina, Ulf-Dietrich Reip, Stefan Stieger, Adam Joinson, & Tom Buchanan. 2007. Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies* 65:526-536.

Pekka, Aula 1999. Chaos, Communication, and Cultural Change: Beyond the Management of Organization in *Managing Complexity in Organizations* edited by Michael R. Lissack and Hugh P. Gunz. Westport CT, Quorum Books 180-196.

Privacy International. 2007. *A Race to the Bottom: Privacy Ranking of Internet Service Companies*. Available at: www.privacyinternational.org. (Retrieved October 19, 2008).

Schell, Bernadette & John Dodge. 2002. *The Hacking of America*. Westport CT: Quorum Books.

Solove, Daniel. 2004. *The Digital Person*. New York NY: New York University Press.

Solove, Daniel. 2008. *Understanding Privacy*. Cambridge MA: Harvard University Press.

Stacey, Ralph. 2007. *Strategic Management and Organisational Dynamics*. 5th Ed. Harlow, England: Prentice Hall.

Tavani, Herman. 2007. Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy. *Metaphilosophy* 38(1):1-22.

Wafa, Tim. 2008. *Today's Inefficient and Impotent Global Internet Privacy Rights Regime & Tomorrow's Inferior Alternative* Available at: http://works.bepress.com. (Retrieved October 19,2008).

Walby, Sylvia. 2003. *Modernities/Globalisation/Complexities*. Paper presented to conference of the British Sociological Association, University of York. York, England.

Warren, Samuel & Louis Brandeis. 1890. The Right To Privacy. *Harvard Law Review* 4(5):193-220.

Westin, Alan. 2003. *Social and Political Dimensions of Privacy*. Journal of Social Issues 59(2): 431-453.

APPENDIX 1: PIPEDA

This appendix documents how the provisions of the privacy legislation (PIPEDA) were transformed so that they could be used to evaluate the privacy policies. Each of the following tables represents one of the ten clauses of Schedule 1 of PIPEDA. The first column gives the rational for the clause; the second describes the sub-clauses; the third provides a quantitative measure for each sub-clause; and the fourth gives the value for the measure (i.e., yes/no or open).

Principle 1 — Accountability	Sub-clause	Measure	Response
An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.			
4.1.1	Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).	name of Privacy Officer (or equivalent)	yes (name) / no
4.1.2	The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.	name of person who oversees compliance available by request (beyond scope of analysis)	
4.1.3a	An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing.	organization accepts responsibility for safe-keeping of personal info	yes / no
4.1.3b	The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.	equivalent protection data transferred to 3rd parties guaranteed	yes / no
4.1.4	Organizations shall implement policies and practices to give effect to the principles, including:		
4.1.4a	(a) implementing procedures to protect personal information;	procedure to protect personal info. stated	yes / no
4.1.4b1	(b) establishing procedures to receive and respond to complaints and inquiries;	mechanism to make a complaint (regarding personal info.) included;	yes (address, telephone, ect.) / no
4.1.4b2		guarantee of response	yes / no
4.1.4c	(c) training staff and communicating to staff information about the organization's policies and practices; and	privacy policies are communicated with staff	yes / no
4.1.4d	(d) developing information to explain the organization's policies and procedures.	(electronic) privacy policy or privacy procedure	yes / no

Principle 2 — Identifying Purposes	Sub-clause	Measure	Response
The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.			
4.2.1	The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).	organization has a privacy policy beyond the electronic public version	yes / no
4.2.2	Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfill these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.	only necessary info. collected (compare to the purpose)	yes / no
4.2.3	The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.	purpose for collection of personal info. stated before/time of collection	yes (negative, check-box) / no
4.2.4	When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).	states that consent for additional uses of personal info. collected before use	yes / no
4.2.5	Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.	if emailed/called, representative would be able to explain purpose (beyond scope of analysis)	
4.2.6	This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).	n/a	

Principle 3 — Consent	Sub-clause	Measure	Response
The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.			
4.3.1	Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).	consent obtained for collection and use of personal info.	yes / no
4.3.2	The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.	"reasonable" effort; "meaningful" consent	"reasonable" = number of clicks, size of font. "meaningful" = reading score
4.3.3	An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes.	consent is given for the specified and legitimate purpose	are there any mandatory fields that would prevent you getting the product
4.3.4	The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.	is the information collected "sensitive" (i.e., reasonable need for privacy?)	yes (what info.?) / no
4.3.5	In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual’s name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual’s request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.	statement of additional purposes for the personal info. collected	yes / no

4.3.6	The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).	consent for information "like to be considered sensitive" obtained?	yes/no
4.3.7	Individuals can give consent in many ways. For example:		
4.3.7a	(a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;	online form?	yes / no
4.3.7b	(b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;	checkbox?	yes / no
4.3.7c	(c) consent may be given orally when information is collected over the telephone; or	telephone?	yes / no
4.3.7d	(d) consent may be given at the time that individuals use a product or service.	at use of product/service?	yes / no
4.3.8	An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.	mechanism for withdrawing consent stated	yes / no

Principle 4 — Limiting Collection	**Sub-clause**	**Measure**	**Response**
The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.			
4.4.1	Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).	personal info. collected matches purpose	yes / no
4.4.2	The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.	stated purpose for collection is not "misleading or deceiving" (beyond scope of analysis)	n/a
4.4.3	This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).	n/a	

Principle 5 — Limiting Use, Disclosure, and Retention	Sub-clause	Measure	Response
Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.			
4.5.1	Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).	repeats 4.2.4	
4.5.2	Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.	states retention times for personal info.	yes (time frame) / no
4.5.3	Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.	states when personal info. is destroyed; organizational policy states when personal info. is destroyed	yes / no
4.5.4	This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).	n/a	

Principle 6 — Accuracy	Sub-clause	Measure	Response
Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.			
4.6.1	The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.	procedure in place to insure accuracy, completeness, and up-to-datedness of info.	yes / no
4.6.2	An organization shall not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.	info. is not routinely updated unless required to fulfill original purpose	yes / no
4.6.3	Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.	info sent to third parties is updated	yes (open) / no

Principle 7 — Safeguards	Sub-clause	Measure	Response
Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.			
4.7.1	The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.	states that personal information is protected by specific safeguards	yes (passwords, encryption) / no
4.7.2	The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.	is protection (4.7.1) consistent with sensitivity of info. (4.3.4)?	yes / no
4.7.3	The methods of protection should include:		
4.7.3a	(a) physical measures, for example, locked filing cabinets and restricted access to offices;	statement of physical protection measures?	yes / no
4.7.3b	(b) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and	statement of organizational measures?	yes / no
4.7.3c	(c) technological measures, for example, the use of passwords and encryption.	statement of electronic measures?	yes / no
4.7.4	Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.	organizational policy is communicated to staff	yes / no
4.7.5	Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).	statement to the provisions to protect personal info. when it is being destroyed	yes / no

Principle 8 — Openness	Sub-clause	Measure	Response
An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.			
4.8.1	Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.	policy is available online ("reasonable" effort for web based organizations)	yes / no
4.8.2	The information made available shall include:		
4.8.2a	(a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;	repeats 4.1.2	
4.8.2b	(b) the means of gaining access to personal information held by the organization;	repeats 4.1.4	
4.8.2c	(c) a description of the type of personal information held by the organization, including a general account of its use;	description of personal info. held	yes (description) / no
4.8.2d	(d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and	repeats 4.1.4	

4.8.2e	(e) what personal information is made available to related organizations (e.g., subsidiaries).	description of what personal info. is released to related organizations	yes (description) / no
4.8.3	An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.	privacy policy available in other (non-electronic) forms	yes (method) / no

Principle 9 — Individual Access	Sub-clause	Measure	Response
Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information.			
4.9.1	Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.	repeats 4.1.4	
4.9.2	An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.	states information required to access personal info. accounts	yes (type of info.) / no
4.9.3	In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.	list of third parties who receive info.	yes / no
4.9.4	An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.	time frame for requests stated; cost of request stated; form of info. stated	yes (days, hours, ect., open) / no
4.9.5	When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.	organization mends inaccuracies	yes / no
4.9.6	When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.	procedure for dealing with unresolved complaints stated	yes / no

Principle 10 — Challenging Compliance	**Sub-clause**	**Measure**	**Response**
An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.			
4.10.1	The individual accountable for an organization's compliance is discussed in Clause 4.1.1.	repeats 4.1.1	
4.10.2	Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.	repeats 4.1.4; procedure for complaining is "accessible" and "simple" "accessible" = stated in privacy policy	yes / no
4.10.3	Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.	procedure for dealing with complaints stated	yes / no
4.10.4	An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.	assurances of investigation of complaints given; assurance that changes made if complaint valid (beyond scope of analysis)	yes / no; n/a